

Державний вищий навчальний заклад
Донецький національний технічний університет
Кафедра прикладної математики та інформатики

«ЗАТВЕРДЖУЮ»

Перший проректор

_____ Леонід БАЧУРІН

«_____» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОК -17 ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальності

125 Кібербезпека

122 Комп'ютерні науки

123 Комп'ютерна інженерія

(шифр і назва спеціальності (тей))

Освітні програми

Кібербезпека

Комп'ютерні науки

Комп'ютерна інженерія

(назва освітньої програми)

Мова навчання: українська

Робоча програма навчальної дисципліни «Основи інформаційної безпеки»
 (повна назва дисципліни)
 для здобувачів вищої освіти за спеціальностями 125 Кібербезпека
 122 Комп'ютерні науки
 123 Комп'ютерна інженерія
 «30» 08 2023 року. – 8 с.

Розробник:
 Володимир МАСОЛ, д.ф.-м.н., проф., професор кафедри ПМІ

Робоча програма затверджена на засіданні кафедри прикладної математики та інформатики

Протокол № 8 від “31” серпня 2023 р.

Завідувач кафедри прикладної математики та інформатики

_____ (Наталія МАСЛОВА)

“31” серпня 2023 р.

Схвалено науково-методичною комісією галузі знань 12 Інформаційні технології

Протокол № 5 від “ 1” 09 2023р.

Голова _____
 (підпис)

(Євген БАШКОВ)
 (прізвище та ініціали)

1. Загальна інформація

Форма навчання	Денна
Статус	Обов'язкова
Обсяг в кредитах ЄКТС	5
Обсяг в годинах за навчальним планом, разом: в тому числі:	150
лекції:	48
лабораторні заняття:	32
самостійна робота:	70
Курсова робота	
Форма підсумкового контролю	Екзамен / диф.залік
Дисципліну викладає	проф. Масол В.І., volodymyr.masol@donntu.edu.ua

Передумови для вивчення дисципліни: перелік дисциплін, які мають бути вивчені раніше: Вища математика, Дискретна математика, Основи алгоритмізації, Програмування.

2. Мета вивчення навчальної дисципліни

Метою вивчення навчальної дисципліни є оволодіння знаннями та вміннями, які утворюють теоретичний і практичний фундамент, необхідний для забезпечення інформаційної безпеки в будь-яких сферах діяльності держави, людини та суспільства.

Компетентності:

- ЗК05. Здатність до пошуку, оброблення та аналізу інформації
- ФК01. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки
- ФК02. Здатність до використання інформаційно - комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки
- ФК03. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах

Програмні результати навчання:

- ПРН12. Розробляти моделі загроз та порушника
- ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.
- ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

- ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем
- ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

3. Очікувані результати навчання

Результатами навчання є наявність базових знань в галузі кібербезпеки, володіння та вільне застосування понять та засобів з інформаційної безпеки.

4. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання є:

- екзамени;
- презентації результатів виконаних завдань;
- виступи на студентських конференціях;
- виконання курсової роботи;
- інші види індивідуальних та групових завдань.

5. Критерії оцінювання результатів навчання

Критерії оцінювання мають формулювати порядок оцінювання під час поточного контролю (за результатами практичних, лабораторних, семінарських занять та виконання індивідуальних або групових завдань) та підсумкового контролю.

ЛР1	ЛР2	ЛР3	ЛР4	ЛР5	ЛР6	ЛР7	ЛР8	Поточний контроль	Іспит	Максимальний бал
5	5	5	5	5	5	5	5	40	60	100
3	3	3	3	3	3	3	3	24		84

Примітка: ЛР1, ЛР2 і т.д. - лабораторні роботи;

В оцінку поточного контролю з виконання практичних робіт включено контрольні та поточні опитування.

Контроль виконання курсової роботи включає поточний контроль за виконанням розрахунків та захист перед комісією. Оцінка виконання та захисту курсової роботи проводиться за 100-бальною шкалою.

Приклад розподілу балів, які отримують студенти за виконання курсової роботи

Пояснювальна записка	Захист роботи	Сума
40	60	100

Захист роботи має на увазі наявність презентації (10 балів) та доповіді (до 50 балів)

Результати підсумкового контролю оцінюються за 100-бальною шкалою та чотирибальною («відмінно», «добре», «задовільно», «незадовільно»).

Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену, курсового проекту(роботи), практики, диференційованого заліку, кваліфікаційного екзамену, випускної кваліфікаційної (дипломної) роботи (проекту)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

6. Програма навчальної дисципліни

6.1. Основні теми дисципліни

Тема 1. Основні поняття інформаційної безпеки

Тема 2. Поняття інформації в інформаційній безпеці

Тема 3. Законодавчий рівень інформаційної безпеки – стандарти, засади та методи забезпечення інформаційної безпеки України

Тема 4. Міжнародні стандарти в інформаційній безпеці. Помаранчева книга – перший оціночний стандарт безпеки

Тема 5. Основні поняття криптології, криптографії та криптоаналізу

Тема 6. Математичні основи криптографічних алгоритмів

Тема 7. Криптографічні методи захисту. Симетричні криптосистеми

Тема 8. Криптографічні методи захисту. Асиметричні криптосистеми

Тема 9. Принципи управління ключами. Поняття хеш-функції та ЕЦП

Тема 10. Основні принципи квантової криптографії

Тема 11. Концептуальна модель безпеки інформації, загрози та вразливості

Тема 12. Модель порушника інформаційної безпеки

Тема 13. Основні поняття теорії ризиків. Керування ризиками та ПЗ аналізу ризиків

Тема 14. Технічні канали витоку інформації.

Тема 15. Шкідливе програмне забезпечення, вірусні атаки

Тема 16. Атаки на операційні системи. Основні атаки на Windows

Тема 17. Мережеві атаки та системи віддаленого доступу

Тема 18. Системи захисту інформації

Тема 19. Ідентифікація та автентифікація. Керування доступом.

Тема 20. Біометрична ідентифікація

6.2. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
1	Лабораторна робота 1. Вступ до інформаційної безпеки	2	
2	Лабораторна робота 2. Частотний аналіз у криптографії	2	
3	Лабораторна робота 3. Елементи теорії чисел в захисті інформації	4	
4	Лабораторна робота 4. Алгоритми пошуку простих чисел	4	
5	Лабораторна робота 5. Шифрування в симетричних криптосистемах	4	
6	Лабораторна робота 6. Шифрування в асиметричних криптосистемах	4	
7	Лабораторна робота 7. Управління ключами	6	
8	Лабораторна робота 8. Біометрична ідентифікація (реферат)	6	
	Усього годин	32	

6.3. Теми практичних занять

Проведення практичних занять не передбачено навчальним планом дисципліни

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
1	Тема 1-2. Історія розвитку та становлення інформаційної безпеки	4	
2	Тема 3-5. Нормативно-правове регулювання діяльності у галузі криптографічного захисту інформації.	6	
3	Тема 6. Сучасні напрямки розвитку криптографії та криптоаналізу	4	
4	Тема 7. Застосування теорії чисел в захисті інформації.	4	
5	Тема 8. Сфери застосування симетричних криптографічних систем.	4	
6	Тема 9. Застосування асиметричних криптографічних систем	4	
7	Тема 10. Додаткові методи криптоаналізу..	4	
8	Тема 11-12 Криптологічні конкурси та змагання. Форми проведення та значення.	6	
9	Тема 13-15. Взаємодія та взаємо доповнення понять ризиків та погроз інформаційної безпеки	6	
10	Тема 16. Придбання навичок з роботи з системами захисту інформації та розрахунку ризиків. Пакет Digital Security	4	
11	Тема 17. Технічні канали витоку інформації.	4	
12	Тема 18-20. Способи захисту програм від шкідливого ПЗ	6	
13	Тема 21. Системи управління інформаційною безпекою та захисту інформації	4	
14	Тема 22-23 Ідентифікація та автентифікація	6	
15	Тема 24. Перспективи розвитку технологій інформаційної безпеки та забезпечення інформаційної безпеки України	4	
Усього годин		70	

6.5. Індивідуальні та/або групові завдання

У рамках курсу студенти виконують курсову роботу з дисципліни. Тематика роботи: «Методи та засоби захисту інформації».

Варіанти завдань обираються згідно номеру в журналі Обліку успішності студентської групи.

Оцінка виконання та захисту курсової роботи проводиться за 100-бальною шкалою.

7. Література

7.1.Основна

1. Бабак, В.П. Інформаційна безпека та сучасні мережеві технології. Англо-українсько-російський словник термінів : Information Security and Modern Network Technology. English-Ukrainian-Russian Dictionary of Terms / В.П. Бабак, О.Г. Корченко . — К. : НАУ, 2013 . — 670 с
2. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. — К., 2013. — 435 с.,
3. Дудикевич, В.Б. Забезпечення інформаційної безпеки держави : навч. посіб. / [В.Б. Дудикевич, П.І. Опірський, В.С. Гаранюк та ін.] . — Львів : вид-во Львівської політехніки, 2017 . — 204 с.
4. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. —КІВіП НУ "ОЮА", кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. — 128 с.
5. Лісовська, Ю.П. Інформаційна безпека України : навч. посіб. / Ю.П. Лісовська . — Київ : вид-во Кондор, 2018 . — 172 с.
6. Лісовський, П.М. Безпекознавство : навч. посіб. : особистість, держава, суспільство (системний аналіз) . — Київ : вид-во Кондор, 2017 . — 368 с.
7. Мінаєв Г.А. Безпека організації. Посібник. Логос, Університетська книга, 2018. — 440с
8. Нашинець-Наумова А.Ю. Практикум з інформаційного права: навчально-методичний посібник / А.Ю. Нашинець-Наумова. — К.: , 2014. — 20 с.

7.2 Допоміжна

9. Вараксін, О.О. Кібербезпека мереж наступного покоління : Навч. посіб. у галузі знань 1701 "Інформаційна безпека" за спеціальністю 8.17010201 - Системи технічного захисту інформації, автоматизація її обробки / О.О. Вараксін, Є.В. Васіліу, С.М. Горохов та ін. ; ред. В.Г. Кононович . — Одеса, 2013 . — 240 с.
10. Голев, Д.В. Методика оцінки інформаційної захищеності телекомунікацій : Навч. посіб. галузі знань 1601, 1701 "Інформаційна безпека" за спеціальністю 7.17010201, 8.17010201 - Системи технічного захисту інформації, автоматизації її обробки / Д.В. Голев, В.Г. Кононович, С.В. Хомич ; ред. В.Г. Кононович . — Одеса, 2013 . — 218 с.
11. Горохов, С.М. Інформаційна безпека цифрових програмно-керованих АТС : навч. посіб. : для студ. вищ. навч. заклад., які навчаються за напрямом "Системи захисту інформаційних та інформаційно-комунікаційних систем" / , В.Г. Кононович, С.В. Стайкуца та ін. — Одеса, 2013 . — 244 с.
12. Сідак В.С., Артемов В.Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС. навч. посібник для студентів вищих навч. Закладів. — К.: КНТ, 2007. — 160с.
13. Denning D. Cryptography and data security. Addison- WesleyPublishing Company. 1982. — 400 p.
14. Jackson K., Hruska J. (Ed.) Computer Security Reference Book.Butterworth-Heinemann Ltd., 1992. — 932 p.
15. Russel D., G.T.Gangemi Sr. Computer Security Basics. — O`Reilli &Associates, Inc., 1991. — 448 p.

7.3 Методична

1. Методичні вказівки для самостійної роботи студентів з дисципліни «Основи інформаційної безпеки» для студентів спеціальності 125 Кібербезпека усіх форм навчання [Електронний ресурс] / укладач Н.О. Маслова, О.І. Патрушева . — Покровськ, 2019 . — 49 с

код НТБ ДонНТУ: М626, М625, режим доступу

http://89.185.3.253:9080/list.php?reallist=2&IDlist=Q_1&s_year=up&_id=1601281094746

2. Методичні вказівки до практичних занять з дисципліни «Основи інформаційної безпеки» для студентів спеціальності 125 Кібербезпека усіх форм навчання [Електронний ресурс] / укладач Н.О. Маслова, О.І. Патрушева . — Покровськ, 2018 . — 60 с.

код НТБ ДонНТУ: М571, режим доступу

http://89.185.3.253:9080/list.php?reallist=2&IDlist=Q_1&s_year=up&_id=1601281094746

3. Методичні вказівки до виконання курсової роботи з дисципліни «Основи інформаційної безпеки» для студентів всіх спеціальностей Галузі 12 (заплановано до видання)

8. Інформаційні ресурси

1. О. В. Черевко Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту // Електронне наукове фахове видання "Ефективна економіка" <http://www.economy.nayka.com.ua/?op=1&z=3304>

2. Список нормативних документів щодо інформаційної безпеки в Україні // [електронний ресурс], http://uk.wikipedia.org/wiki/Список_нормативних_документів_щодо_інформаційної_безпеки_в_Україні

3. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про скасування деяких рішень Ради національної безпеки і оборони України» // [електронний ресурс], режим доступу <http://zakon1.rada.gov.ua/laws/show/514/2009>

4. Правові основи захисту інформаційної безпеки в Україні // [електронний ресурс], режим доступу <http://studies.in.ua/inform-pravo-shporu/2530-pravov-osnovi-zahistu-nformacynoyi-bezpeki-v-ukrayin.html>